HARRIS
Electronic Systems

HARRIS CORPORATION
Information Systems Division

JA #1486

Network Visualization Tool (NVT)

Task #3 Report: Comparison of COTS Vulnerability Assessment/Reasoning Engines for Automated Reasoning

October 6, 1998

Contract #F30602-96-C-0289

Mr. Dwayne P. Allain
AFRL/IFGB
425 Brooks Road
Rome, NY 13441-4503

Table of Contents

ABSTRACT: 1

1.0 Introduction 1

2.0 Survey of Vulnerability Assessment and Reasoning Tools 2

3.0 Tool Evaluation Criteria 2

4.0 Selection Process 6

5.0 Recommendation 9

Appendix A - Vulnerability Assessment Technologies Summary 1

ABSTRACT:

This paper documents the findings of Task Three - Automated Reasoning of the Network Visualization Tool (NVT) program. Task Three, Automated Reasoning, identified and evaluated available commercial-off-the-shelf (COTS), government-off-the-shelf (GOTS), and evolving research vulnerability assessment and reasoning tools for applicability as integrated automated reasoning engines for the NVT program prototype. The evaluation criteria included assessment capability, output type, type of vulnerability assessed, data acquisition method, platform operability, and applicability for the NVT program prototype. Three vulnerability assessment reasoning tools, reflecting three different types of reasoning engines, are recommended for inclusion in the NVT prototype.

1.0 Introduction

The Network Visualization Tool program is based on the concept of a knowledge solicitation framework that incorporates a graphical description of a network topology. This topology is used for capture of network attributes, and is subsequently analyzed for security vulnerabilities. The knowledge solicitation portion of NVT uses modern network discovery capabilities and a graphical user interface to increase the accuracy of the network model, provides a common network description for multiple risk analysis reasoning engines, and enhances the productivity of the system security analyst. The NVT program should provide a single topological model supporting the information needs of multiple reasoning tools. In addition to collecting information for input into the reasoning tools, NVT can be used to highlight the vulnerabilities identified by the various reasoning tools. Therefore it is desirable that the vulnerability assessment and reasoning tools have data acquisition and data output formats that are easily adapted to knowledge solicitation portion of NVT.

NVT Task Three-- Automated Reasoning surveyed the current vulnerability assessment and reasoning tools to determine their capabilities and availability. These tools were categorized by the types of vulnerabilities assessed and the functional tool characteristics. Each tool was further evaluated on its data acquisition and output formats to determine how the information can be applied in the NVT prototype implementation. The trade survey methodology is outlined in Section 2.0 of this paper. The characterizations developed during the evaluation are described in Section 3.0 of this paper. Section 4.0 describes the selection process and the criteria used. Section 5.0 recommends three vulnerability assessment and reasoning tools for inclusion in the NVT prototype. The surveyed vulnerability assessment technologies are summarized in Appendix A.

2.0 Survey of Vulnerability Assessment and Reasoning Tools

A trade survey of existing vulnerability assessment and reasoning tools was conducted to determine the scope of capabilities available for inclusion in the NVT prototype. The tools surveyed included:

- •Government-Off-The-Shelf (GOTS) tools, which were developed under Government contracts and are used for vulnerability assessment without additional tailoring as a "standard" capability.
- •Commercial-Off-The-Shelf (COTS) products, which are sold for immediate application and maintained as commercial products, available on the open market.
- • Research tools, which are still in the laboratory with varying phases of maturity.

Various methods were employed to identify the available vulnerability assessment and reasoning tools and to gather specific data on the tools. The methods and their results are summarized in Table 1, Survey Methods.

Table 1, Survey Methods

Method	Result
Internet search (various engines)	Voluminous and somewhat redundant data
Trade show attendance (MIS Institute/ISSA Open Systems Security Exposition, Orlando, FL (Date)	Clarification and vendor information on the most popular COTS products.
Trade Publications (Federal Computer Week, Internet Week, Network World, Information Security, Information Security Product News)	Multiple leads and vendor contact data, resulted in product literature, vendor discussion.
Canvas of Professional Associates	Additional Research Tools, unpublicized GOTS tools
Evaluation Copies (Risk Watch, Buddy System, Net Auditor)	Hands-on product assessment

The surveyed vulnerability assessment and reasoning tools with their NVT prototype relevant characteristics are summarized in Appendix A.

3.0 Tool Evaluation Criteria

The functional evaluation criteria used to select the vulnerability assessment and reasoning tools were selected to facilitate tools integration into the NVT prototype. The primary criteria were the operating system required by the tool, the capability of the tool to assess network environments, the data gathering methods used by the tool, and the risk types assessed by the tool. The surveyed tools varied greatly in their ability to meet the functional criteria. .

The vulnerability assessment and reasoning tools have to be able to run in the NVT prototype's operational environment consisting of the hardware platform and operating system. The required platforms were identified as one or more of the following operating systems; PC/DOS, Windows, MAC, UNIX, and WindowsNT.

For the NVT prototype to have the capability to assess the vulnerabilities and risks associated with a network or distributed system environment, the vulnerability assessment and reasoning tools need to be able to understand the vulnerabilities of an networked communications environment. In this evaluation, this criteria is termed 'Network Smart'. Initially this characteristic was defined as the capability to identify and assess network functions and components. Many of the COTS tools were originally developed for independent systems or systems with limited connectivity and were not considered "Network Smart". Further research indicated some of the tools could be configured to recognize basic network functions and components.

The NVT framework model is envisioned as interactively providing data to the vulnerability assessment and reasoning tools and synthesizing the result data received from the tools. Therefore, the methods by which the tools were designed to collect input data and the method and formats used to report result data were identified as key criteria.

The method of data collection was categorized as active or passive. The active method of data input:

- uses agent software for monitoring activity on the system,
- performs interactive traffic analysis for determining system structure,
- and may query identified nodes for connectivity, protocols, and users.

Active data gathering methods can be further decomposed into either active or active resident technologies. The active method is the predominant type used in the vulnerability assessment and reasoning tools. The active method gathers information only on the current state of the system being assessed, i.e., a single snap shot of the system being assessed. In the active resident method, the agent software remains persistent after the initial state is assessed and continues to monitor for additional activities and/or changes. This type of data gathering can provide ongoing analyses and some intrusion detection capabilities. This continuing assessment capability incurs a greater integration complexity for the NVT prototype.

The passive method of data input is:

- predominately user intensive
- characterized by system defined inputs configured during tool installation
- user inputs from questionnaire, and/or selectable inputs from a predefined data base.

Many of these tools were developed with an emphasis on the tool's reasoning and analysis capabilities and not on user friendly or automated data acquisition methods. While cumbersome to integrate into the interactive NVT framework, some of these tools are highly flexible and can accommodate diverse target system configurations.

Output characteristics of the tools were expressed in terms of:

- risk matrices identifying types of risks identified, e.g., system risk, component risk, operating system risk, etc,
    - annualized expected financial loss based on statistical probability of an identified vulnerability being exploited times the dollar value of the resource compromised,
- criticality of components defining the relative risk and the degree of risk that each component exposes the system to,
- compliance reports based on data gathered compared to a defined set of requirements,
- risk over time stated as a statistical probability of an occurrence during a given period of time.

None of the tools possessed configurable or tailorable output characteristics.

The last major functional criterion was the risk type analyzed by the vulnerability assessment and reasoning tool. While the supported operating systems and data gathering methods were definitive, concrete criteria, the risk types addressed by the tools varied greatly from identifying the risk in only general terms to identifying specific risks associated with individual functions to an infinite range of user defined risks. Having been developed for the commercial environment, many of the tools expressed risk in terms annualized financial loss expectancy.

The functional selection criteria for vulnerability assessment and reasoning tools are summarized in Table 2, Functional Criteria.

Table 2, Functional Criteria

Characteristic	Definition/Rationale
Platform/Operating System: This refers to the platform(s) and operating system(s) in which this tool can run.	The tool has to be able to run on the NVT prototype platform. Unique or additional environmental support software or hardware are more likely to result in later compatibility and integration problems when additional reasoning tools are incorporated into NVT.
Product/Research: The source and developmental status of the tool.	The availability of support for a tool is most likely from a commercial vendor. Additionally, the more mature a tool is the less likely modification will adversely affect the tool's integration into the NVT prototype.
Risk Types Considered in the Analysis: The types of risk that the tool evaluates.	The tools should include a comprehensive selection of risk types to be analyzed.
Information Gathering Method: The tool's data acquisition methods.	A tool with a passive data acquisition method is associated with system defined inputs, user questionnaire inputs, user selectable inputs from a generic data base, or any combination of these methods. An active data acquisition technology is associated with agent software monitoring activity on the system, performing traffic analysis for determining system structure and connectivity, querying identified nodes for connectivity, protocols, users, etc, or any combination of these methods. An active resident technology, after identifying the system parameters using any of the 'active' methods, remains persistent, continuing to monitor for additional activities and/or changes, and provides ongoing analyses. Finally, a tool may possess a combination of active, passive, and active resident technologies.
Risk Metric Expressed in terms of: The data output capability of the tool to provide relevant analysis data for the NVT prototype.	The output data of reasoning tools will be used by the NVT prototype for fusion with other tool's outputs into a cohesive, consolidated output. In order to provide a comprehensive view of the network under evaluation, the prototype requires as many different risk analyses types as possible

IW Smart: The capability of the tool to employ Information Warfare technologies and/or recognize offensive or defensive techniques.	If a reasoning tool possessed IW technologies its inclusion in the NVT prototype would be facilitated. Please explain what an IW technology is, this criteria isn't mentioned in the textual explanation.
Network Smart: The capability to assess network characteristics.	Many vulnerability assessment and reasoning tools were developed originally for independent monolithic systems or systems with limited connectivity; NOT for a network of systems.
Quantitative / Qualitative: The characterization of the tools output data.	The quantitative tool output can be expressed as a definitive value or a range of values. A qualitative output is expressed in subjective terms such as poor, good, better, best, highly vulnerable, less vulnerable, etc. In order to fuse the reasoning tool's output data, the prototype needs to understand the format and context of the output data.
Asset valuation: Whether the tool expresses risk in terms of financial loss/relative importance of components.	In order for the prototype to rank risks or vulnerabilities, the relative importance of each characteristic/component needs to be established.

4.0 Selection Process

A primary purpose of the NVT prototype is to demonstrate a framework model with the flexibility to integrate and interactively use existing vulnerability assessment and reasoning technologies. The existing COTS, GOTS, and research vulnerability assessment and reasoning tools were surveyed and their characteristics identified. In order to demonstrate the proof of concept within program restrictions, only a representative sample of tools is needed for inclusion in the NVT prototype. These selected tools have to represent the greatest diversity of characteristics while exposing the NVT program to the least amount of integration risks.

The primary consideration for selection was that the tools had to be able to run in the NVT prototype's operational environment without modification. Therefore the selected tools must be compatible with the selected operating system of the NVT prototype. Early in the selection process, WindowsNT was selected as the operating system of choice for the NVT prototype. Windows NT was selected due to its wide availability and acceptance in the target user community. This focused the survey process on the tools capable of running in the WindowsNT, Windows, and possibly the PC/DOS operating system environment. The vulnerability assessment and reasoning tools meeting the operating system requirements are identified in Table3, Tools' Operating System Requirements.

Table 3, Tools' Operating System Requirements

Product Name	Manufacturer information	Product/ Research	PC/DOS	PC/Windows	MAC	WindowsNT	UNIX
Norman Risk Analysis: The Buddy System	Norman Data Defense Systems, Inc. 3040 Williams Drive, 6th Floor Fairfax, Virginia 22031 (703) 573-8802 fax (703) 573-3919 http://www.norman.com/	product	√	√		√	
@ Risk	Palisade Corp, 31 Decker Rd., Newfield, NY 14867 800-432-7475 http://www.palisade.com/	product	√	√	√	√	
RAM Risk Assessment Model	National Security Agency POC Cpt Donald Buckshaw, R52	research		√		√	
PRISM Risk Analysis and Simulation for the PC (Note 1)	Palisade Corp, 31 Decker Rd., Newfield, NY 14867 800-432-7475 http://www.palisade.com/	product		√	√	√	
ANSSR	Mitre Corp Bedford, MA POC: Mr. Fred Chase fnc@mitre.org	research	(Note 2)				
Secure Detector	ODS Networks Inc. Richardson, TX 75024 http://www.ods.com/	product		√		√	
Kane Security Analyst	Intrusion Detection, Inc http://www.intrusion.com/ IDI acquired by Security Dynamics, Bedford, MA http://205.181.76.22/	product		√		√	
ISS Scanner Toolset	Internet Security Systems Atlanta, GA http://www.iss.net/	product		√		√	√
ISS Internet Scanner	Internet Security Systems Atlanta, GA http://www.iss.net/	product		√		√	√
WebTrends Security Analyzer (Previously named Asmodeus)	WebTrends Corporation free v2.0 Beta from http://www.webtrends.com/wss/	research/ development		√		√	

Note 1 PRISM has been incorporated into @Risk
Note 2 Smalltalk compatible platforms

A design goal of The NVT analysis framework is support for multiple and varied vulnerability assessment and reasoning tools. To demonstrate this design goal the NVT prototype should include multiple vulnerability assessment and reasoning tools with varied major tool characteristics. Within program time and cost constraints only two, or possibly three, vulnerability assessment and reasoning tools can be incorporated into the NVT prototype.

The selected tools should represent the largest diversity within the major characteristics of data acquisition, output format, and risk types. The selected tools are representative both of the active and passive data acquisition technologies. The active resident data gathering tools are not included because of the complexity associated with assimilating the continuous output data within the NVT prototype. Program constraints dictate that the NVT prototype demonstrate the ability to synthesize the outputs from multiple vulnerability assessment and reasoning tools as a primary objective. Resolving the complexities of continuous data output from a single tool is beyond the present scope of the program. Finally, it is desirable that the selected vulnerability assessment and reasoning tools be capable of analyzing a variety of risk types.

The selection process criteria eliminated from further consideration, those vulnerability assessment and reasoning tools which were not compatible with the WindowsNT operating system and those with active resident data gathering technologies. The remaining tools were evaluated as to their advantages and disadvantages for inclusion in the NVT prototype. This subset of candidate vulnerability assessment and reasoning tools is summarized in Table 4, Tools' Advantages and Disadvantages, enumerating the advantages and disadvantages of each tool.

Table 4, Tools' Advantages and Disadvantages

Product	Platform/ OS	Information Gathering Method	Advantages	Disadvantages
Buddy System	PC/DOS, PC/ Windows	survey	analysis includes networks, stable COTS product,	no risks analyzed only expressed in terms of possible annual loss single level survey input
"@ Risk	PC/DOS, Windows, MAC	User Defined Algorithm	data gathering and risk types analyzed flexible but complex through user defined algorithms	no risks analyzed only expressed in terms of possible non dollar loss does not analyze networks
RAM Risk Assessment Model	PC/Windows	Combination active and passive; partial survey	data gathering through a combination of active and passive methods denial of service risk expressed over time available from another government agency	single type of risk analyzed does not actively identify network vulnerabilities
PRISM Risk Analysis and Simulation for the PC	PC/Windows, MAC	User Defined Algorithm	accommodates simulations of different system configurations	risk expressed only in non dollars does not analyze network vulnerabilities
ANSSR	Smalltalk compatible platforms	survey, Q&A	multiple risk types analyzed multi-level passive input method IW cognizant analyzes network vulnerabilities	research product - possibly limited support
ISS Internet Scanner	WindowsNT, Unix	active, graphical	analyzes network vulnerabilities active data gathering multiple risk types analyzed	risk expressed in compliance report

Only the last entry in the above table, the ISS Internet Scanner, uses an active single state data gathering technology exclusively. All the other gathering vulnerability assessment and reasoning tools have passive data gathering methods or require the use of a combination of passive and active methods.

5.0 Recommendation

A comparison of the functional evaluation criteria required for the NVT demonstration versus those characteristics identified as being available in the seven remaining vulnerability assessment and reasoning tools is shown in Table 5, Tools' Operational Characteristics.

Table 5, Tools' Operational Characteristics

Vulnerability Assessment Tool	WindowsNT Operating System	Active Data Gathering Method	Passive Data Gathering Method	Network Smart	Number of Risk Types Assessed
Buddy System	Yes	No	Yes	Yes	0
"@ Risk	Yes	No	Yes	No	0
RAM Risk Assessment Model	Yes	Yes	Yes	No	1
PRISM Risk Analysis and Simulation for the PC	Yes	No	Yes	No	0
ANSSR	Yes	No	Yes	Yes	multiple
ISS Internet Scanner	Yes	Yes	No	Yes	multiple

Only the ISS Internet Scanner employs a totally active data acquisition method and is considered network smart. Of the other five vulnerability assessment and reasoning tools (Buddy System, "@ Risk, RAM Risk Assessment Model, PRISM Risk Analysis and Simulation for the PC, and ANSSR) identified as having passive data gathering capabilities, RAM Risk Assessment Model, and ANSSR assess specific risk types. ANSSR, RAM Risk Assessment Model, and ISS Internet Scanner are recommended for inclusion in the NVT prototype. These three vulnerability assessment and reasoning tools meet the NVT prototype requirements and provide the greatest diversity of functional capabilities as shown in Table 6, Recommended Tools' Capabilities summary. The final selection of the product used should be made with the endorsement and involvement of the Program Office.

Table 6, Recommended Tools' Capabilities Summary

Recommended Candidate	**Functional Capabilities**
ANSSR (Analysis of Networked Systems Security Risks - Mitre Corporation	Passive data gathering - Model structure - Survey based data gathering - Network aware Risk Type - Single Occurrence of Loss
RAM (Risk Assessment Model) - NSA	Passive data gathering - Event tree - Prioritized attack list Risk Type - Mathematical model - Multiple risks / services - Event based over time Extensible to Risk Type - Comparison of effectiveness of different designs - Not limited to computers/networks - Optimization of system / cost benefit analysis
ISS (Internet Security Systems) Internet Scanner - Internet Security Systems Corporation	Active data gathering - Scans network for hosts, servers, firewalls, and routers - Assesses security and policy compliance of networks, operating systems, and software applications Risk Type - Computer Network Compliance Report (snapshot in time)

Appendix A - Vulnerability Assessment Technologies Summary

The vulnerability assessment and reasoning tools surveyed are summarized in Table A1, Vulnerability Assessment Technologies Summary. The selection WindowsNT as the NVT prototype's operating system restricted the potential tools surveyed to those capable of executing within a WindowsNT environment. In addition to identifying the vulnerability assessment and reasoning tools surveyed, Table A1 summarizes each tool's applicable characteristics. Those characteristics are:

- **Product/ Research -** Product: The tool is available as a COTS product. Research: The tool is available from an organization which developed the tool as a research program and the organization has not offered the tool as a commercial product.

- **Platform/ OS -** This identifies the operating system(s) on which the tool was originally developed and intended to execute.

- **Risk Types considered in analysis -** This identifies which risks the tool analyzes.

- **Information Gathering Method -** This is the method which the tool uses to collect the data necessary to analyze its stated risk types.

1. Survey: A user filled out questionaire(s) for the system being analyzed.
2. Q&A: A user answering questions in an interactive session with the tool.
3. User Defined Algorithm: The method of data gathering varies depending on the user's selection of the tool's capabilities and the degree of granularity desired.
4. Passive, Active, and Active resident: The tool gathers significant portion of data through automated techniques from physical connections to the system being analyzed.
5. Graphical: Interactive user input via a graphical representation.

- **Risk Metric Expressed in terms of -** How the tool defines output of its analysis.

- **IW Smart -** Where or not the tool has the capability to analyze Information Warfare vulnerabilities.

- **Network Smart -** Where or not the tool recognizes and analyzes network vulnerabilities.

- **Quantitative/ qualitative -** How the tool presents the degree of risk associated with each identified vulnerability. Quantitative: e.g., number of vulnerabilities associated with each network node. Qualitative: e.g., risk ranking based on a defined scale.

- **Asset valuation -** Where or not the tool is capable of associating an asset valuation with each vulnerability/risk.

Table A1, Vulnerability Assessment Technologies Summary

Product Name	Manufacturer information	Product/ Research	Platform/ OS	Risk Types considered in analysis	Information Gathering Method	Risk Metric Expressed in terms of	IW Smart	Network Smart	Quantitative / qualitative	Asset valuation
IST/RAMP international Security Technology Risk Analysis Management Program	International Security Technology	product	IBM mainframe w/PC	delay, physical, damage, fraud, unauthorized disclosure	survey, Q&A	single loss occurrence	no	no	Quantitative	partial
BDSS Bayesian Decision Support System	A SYS T Inc.	product	PC/DOS	Asset loss	survey, Q&A	Annualized loss exposure	no	N/A	both	yes
Criti Calc	International Security Technology	product	PC/DOS	data destruction, unavailability	Q&A	Annualized loss exposure	no	no	both	yes
CRAMM CCTA Risk Analysis and Management Methodology	BIS Applied Systems Limited UK	product	PC/DOS	disclosure modification, denial of service, destruction	survey, Q&A	risk ranking	no	no	Quantitative	yes
MicroSecure Self Assessment	Boden Associates	product not supported	PC/DOS	disclosure modification, denial of service, destruction	survey	risk no metrics	no	no	Qualitative	no
GRA/SYS	Small Business Administration Nander & Brown	GFE product	PC/DOS	loss	survey	risk ranking	no	no	Qualitative	no
ALRAM Automated Livermore Risk Analysis Methodology	Expert-Ease Systems	product	PC/DOS	N/A	survey	risk ranking	N/A	N/A	Quantitative	yes
Control It	Jerry Fitzgerald and Assoc.	Product	PC/DOS	N/A	Q&A	risk ranking	no	partial	Quantitative	no
RA/SYS	Small Business Administration Nander & Brown	GFE product	PC/DOS	N/A	survey	Risk Ranking & Expected Loss	N/A	N/A	Quantitative	yes
Rank It	Jerry Fitzgerald and Assoc.	product	PC/DOS	N/A	Q&A	Risk Ranking	no	partial	Quantitative	no
RiskPAC	Computer Security Associates	product	PC/DOS	N/A	survey	Annualized loss exposure, dollar and nondollar	N/A	N/A	both	yes

Table A1, Vulnerability Assessment Technologies Summary - Continued

Product Name	Manufacturer information	Product/ Research	Platform/ OS	Risk Types considered in analysis	Information Gathering Method	Risk Metric Expressed in terms of	IW Smart	Network Smart	Quantitative / qualitative	Asset valuation
RiskWatch	Expert Systems Software	product	PC/DOS	N/A	survey, Q&A	Annualized Loss Exposure	partial	yes	both	yes
SOS Security Online System	Entellus Technology Group	product	PC/DOS	N/A	survey	Annualized Loss Exposure	partial	partial	both	yes
ARES Automated Risk Evaluation System	AF contractor for AFCSC/SR	research	PC/DOS	OPSEC	survey	Risk listing	no	no	Quantitative	yes
Janber	Eagon, McAllister Associates, Inc	Product unsupported	PC/DOS	OPSEC	survey, Q&A	risk ranking	no	no	Quantitative	no
MARION	Cooper & Lybrand UK	product	PC/DOS	OPSEC	survey	scaled risk	no	no	Quantitative	no
MINIRISK	Small Business Administration Nander & Brown	GFE product	PC/DOS	OPSEC	survey	scaled risk	no	no	Qualitative	no
LLAVA Los Alamos Vulnerability and Risk Assessment	Barranca Inc	product	PC/DOS	OPSEC LAN, PC	survey, Q&A	scaled risk	some	yes	Qualitative	N/A
CONMAT Control Matrix	Small Business Administration Nander & Brown	GFE product	PC/DOS	single machine application	survey	risk ranking	no	no	Qualitative	no
RiskCALC	Hoffman Business Associates	product	PC/DOS	loss	survey	Annualized loss exposure, dollar and nondollar	no	no	Quantitative	yes
Buddy System	Norman Data Systems	Product	PC/DOS, PC/ Windows	N/A	survey	Annualized loss exposure	N/A	yes	Qualitative	yes
"@ Risk	Palisade Corp, Newfield	Product	PC/DOS, Windows, MAC	User Defined Algorithm	User Defined Algorithm	Expected Loss (non-dollar)	N/A	N/A	Quantitative	N/A
RAM Risk Assessment Model	NSA	research	PC/ Windows	denial of "service"	partial survey	risk over time	no	no	both	no

Table A1, Vulnerability Assessment Technologies Summary - Continued

Product Name	Manufacturer information	Product/ Research	Platform/ OS	Risk Types considered in analysis	Information Gathering Method	Risk Metric Expressed in terms of	IW Smart	Network Smart	Quantitative / qualitative	Asset valuation
PRISM Risk Analysis and Simulation for the PC	Palisade Corp, Newfield	product	PC/ Windows, MAC	User Defined Algorithm	User Defined Algorithm	Expected Loss (non-dollar)	no	no	Quantitative	N/A
ANSSR	Mitre Corp	research	Smalltalk compatible platforms	Network, unauthorized disclosure, denial of service	survey, Q&A	single loss occurrence	partial	yes	Quantitative	yes
VISART Risk Analysis, Confidentiality & Extending Expected Value	NSA	research	unk	multiple risks	unk	aggregate risks for protecting critical assets	unk	unk	both	unk
Secure Detector	ODS Networks Inc.	product	Windows NT	intrusion detection	active resident, partial graphical	compliance reports	no	yes	Quantitative	no
Kane Security Analyst	Intrusion Detection, Inc IDI acquired by Security Dynamics	product	Windows NT	unauthorized access, denial of service	active resident, graphical	risk ranking	no	partial	both	no
ISS Scanner Toolset	Internet Security Systems	product	Windows NT, Unix	anomaly detection	active, partial resident; graphical	compliance reports	no	yes	Quantitative	no
ISS Internet Scanner	Internet Security Systems	Product	Windows NT, Unix	Network, o/s, s/w	active, graphical	compliance reports	N/A	yes	Qualitative	no
WebTrends Security Analyzer (formally Asmodeus)	WebTrends Corporation	product - beta	Windows NT	scan IP ports on multiple servers for available services and ipotential weaknesses	active, resident	user defined response	no	yes	Quantitative	no
netformX	netformX, Inc.	product	Windows, NT	network visualization	active	reports	no	no	Qualitative	no
Analyser	Netman Development Group at Curtin University of Technology, Perth, Western Australia	academic release	Unix	configuration optimizer	passive, input from other tools	reports	no	no	Qualitative	no
Argus	Software Engineering Institute, Carnegia Mellon University	public domain generic IP network transaction auditing tool	Unix	audit data reduction	passive, audit data, reading network datagrams	network traffic status records	no	partial	Quantitative	no